Engineering Improvement in Software Assurance: A Landscape Framework

Team:
Lisa Brownsword
Carol C. Woody
Christopher J. Alberts
Andrew P. Moore

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
12 MAY 2010		**00-00-2010 to 00-00-2010**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Engineering Improvement in Software Assurance: A Landscape Framework	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Carnegie Mellon University,Software Engineering Institute,Pittsburgh,PA,15213**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**31**	

About Lisa Brownsword

Sr. Member of the SEI Technical Staff

Research efforts focus on the software assurance, development, and governance aspects for system of system (SoS) environments

20 years of experience in software design, development, and acquisition in large complex organizations

About Carol Woody

Sr. Member of the SEI Technical Staff

Leads a team in CERT addressing critical gaps in assurance and survivability

25 years of experience in software management, acquisition, development, and implementation in large complex organizations

Webinar Instructions

Polling Question 1

How did you hear about this webinar?

a) Email invitation from the SEI
b) SEI website
c) Website with webinar calendar (i.e., www.webinar-directory.com)
d) Social media site (e.g., LinkedIn, Twitter)
e) Other

Agenda

Problem Space

Introduction to the Assurance Modeling Framework

Summary and Questions

Why is modeling important?

Modeling facilitates understanding complexity

- Mechanisms to structure, describe, analyze, and discuss complexity
- Provides a way to describe the range of behaviors of the stakeholders involved
- Provides a way to describe key social and technical elements that must work together to achieve results—a collaboration among solutions and participants

Modeling to understand software assurance

- Numerous assurance solutions (i.e., technologies, policies, and practices) are available
- A large number of organizations produce or fund these assurance solutions
- Unclear how available assurance solutions contribute to resulting operational assurance
- Need for a way to describe differences between available solutions and assurance results (and how to bridge the gaps)

Assurance is More than Requirements Validation

Software assurance

- Justified confidence that software functions as intended and is free of exploitable vulnerabilities, either intentionally or unintentionally designed or inserted at any time during the life of the software

Software context

- Functions as intended: includes user expectation
  - Which will change over time
- Context of use: *actual* operational mission and environment of use
  - Which may or may not be reflected in a requirements artifact

Multiple Models Needed

Question	Method Used to Generate Models
1. How is software assurance value defined for a selected context?	Critical Context Analysis
2. Who/what are the participating organizations and assurance solutions?	Value Mapping
3. What are the elements of value exchanged among participating organizations and assurance solutions?	Value Mapping
4. How do participating organizations and assurance solutions work together to achieve operational assurance?	SoS Focus Analysis
5. What are the drivers and motivations of participating organizations?	Driver Identification and Analysis
6. What are the critical usage scenarios and behaviors among the participating organizations and assurance solutions?	System Dynamics
7. What are the adoption and operational usage mechanisms used for assurance solutions? How are they aligned with organizational contexts and needs?	Technology Development and Transition Analysis
8. What is the impact of future trends and events on participating organizations and assurance solutions?	Strategic Alternatives Analysis
9. What patterns of possible inefficiencies affecting the formation, adoption, and usage of assurance solutions can be identified?	[informal analysis]
10. What are candidates for improvements? What could be the impact, if implemented?	[informal analysis]

A Pilot Using Vulnerability Management

Characteristics of the example

- Operational environments across all domains are plagued with undiscovered defects and escalating numbers of known vulnerabilities
- Management of vulnerabilities includes detection, remediation, and prevention activities
- Success requires the effective interactions of technologies, practices, people, and organizations

Rich set of available solutions, e.g.,

- Common Vulnerabilities and Exposures (CVE)®
- Common Weakness Enumeration (CWE)™
- NIST National Vulnerability Database (NVD)
- Static Analysis (various vendor products)
- Secure coding practices (emerging standards and research)

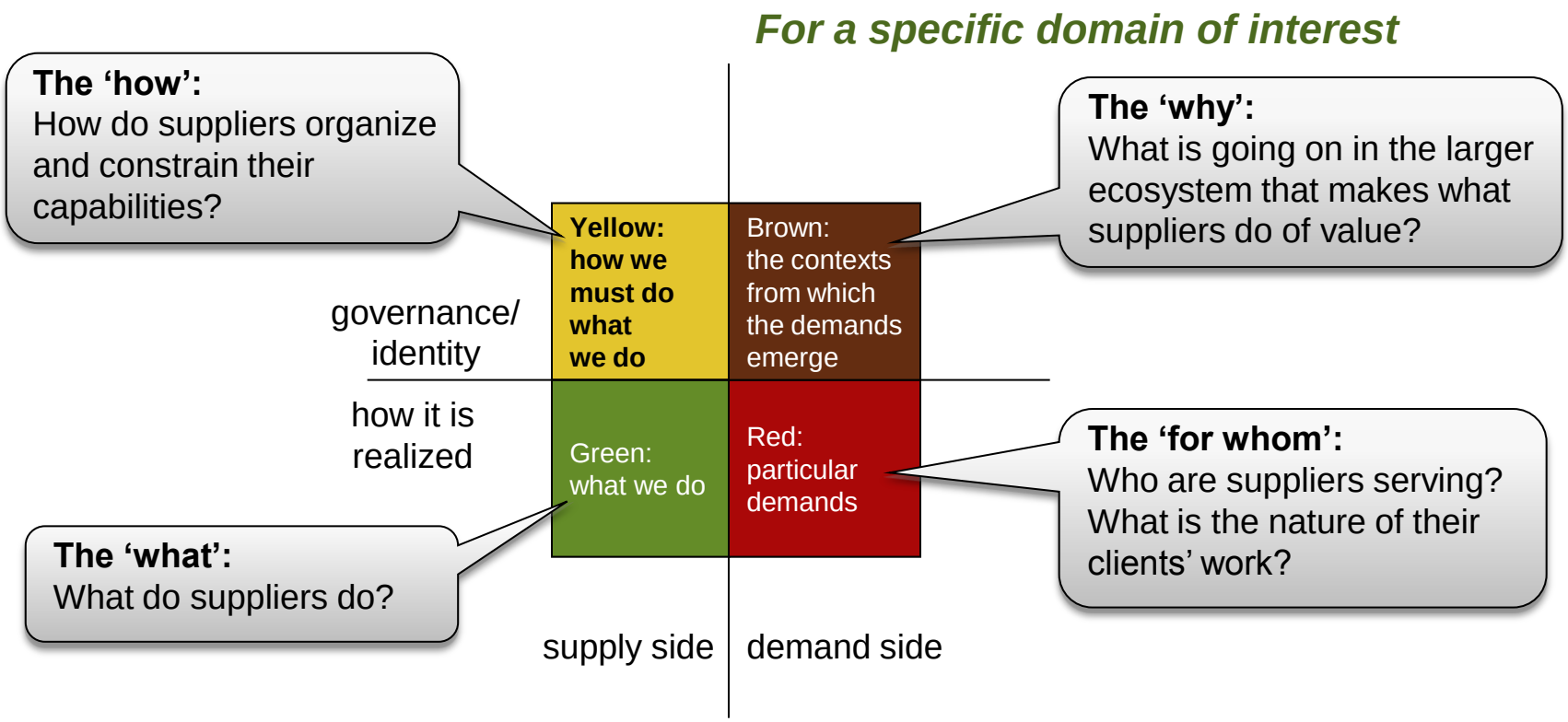
® CVE is a registered trademark of The MITRE Corporation.
™ CWE is a trademark of The MITRE Corporation.

Polling Question 2

Are you familiar with vulnerability management?

a) Very familiar
b) Somewhat familiar with the terms
c) No familiarity

Critical Context Analysis: Principal Perspectives & Influences (Q1, 2)



Critical Context Analysis for CVE

Reveals a broad range of types of organizations with interrelated roles

Domain: CVE Support for Software Vulnerability Management

New vulnerabilities registered in **CVE** list. Vulnerability pattern determined. Vulnerability data added to **NVD**.

CVE board monitors that new vulnerabilities registered in timely fashion.
NIST monitors use of NVD.

Operational organizations of U.S. DoD and government agencies that rely on computers, networks, software applications, data storage media to perform their mission; cannot afford loss of data integrity, data confidentiality, and availability for operations.

governance/ identity

How do suppliers organize and constrain their capabilities?

What is going on in the larger ecosystem that makes what suppliers do of value?

how it is realized

What do suppliers do?

Who are suppliers serving? What is the nature of their clients' work?

SW application vendors: build, test, issue patches for vulnerabilities. Register patches in CVE list.

SW security product vendors: build, test, issue a capability to detect/contain a vulnerability. Cross reference to CVE ID.

supply side: managing vulnerabilities

Site security analysts: track vulnerabilities and available patches; form site specific solutions; and notify IT ops of vulnerabilities and solutions.

IT operations: track and install available site solutions; get computer users to install patches, and monitor for compliance.

demand side: concerned with assurance of operational systems

Value Mapping: Value Exchanged (Q2, 3, 4)

Legend

Symbols

Participant	A participant (e.g., organization or technology) in a value exchange
●	Data source for public information with multiple contributors

Line Style

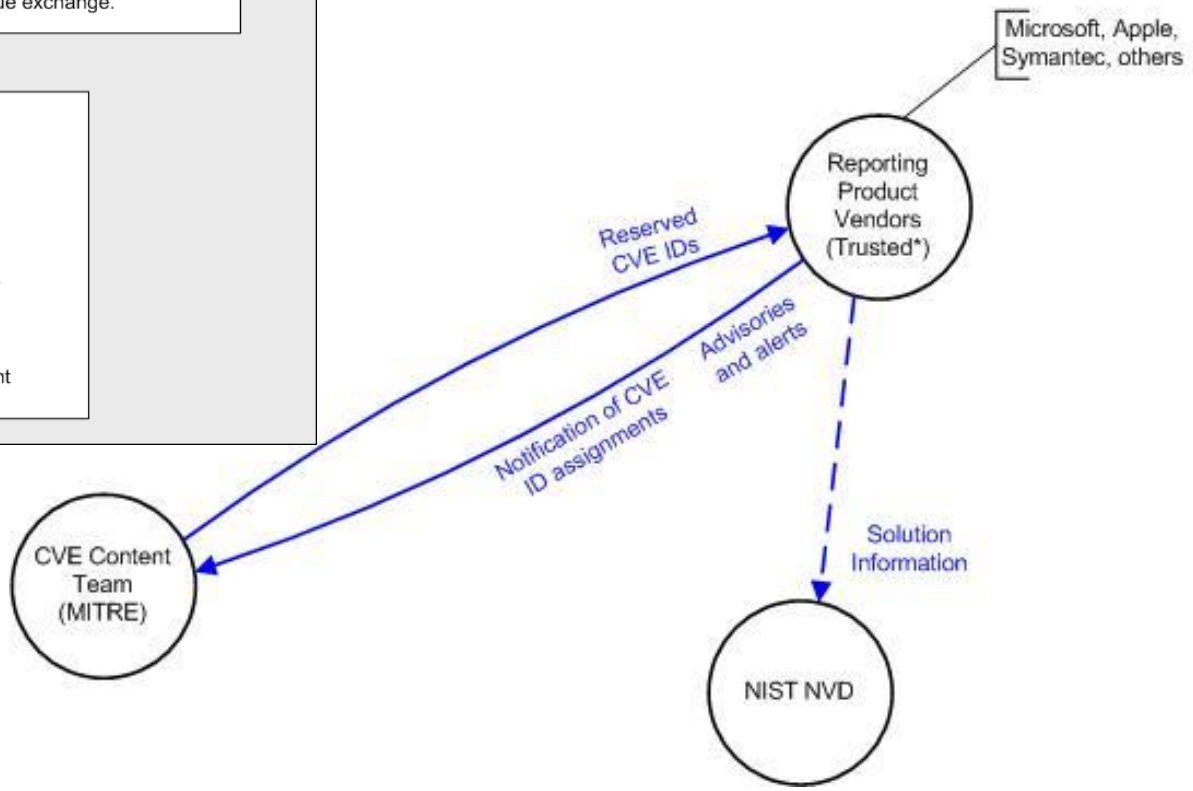
– – – → Dashed arrow	Value is pulled by destination organization.
——→ Solid arrow	Value is pushed from source organization.

Note: The direction of the arrow shows the flow of the value exchange.

Line Colors

Green	Funding
Blue	Product
Brown	Service
Gray	Governance
Red	Compliance
Orange	Endorsement

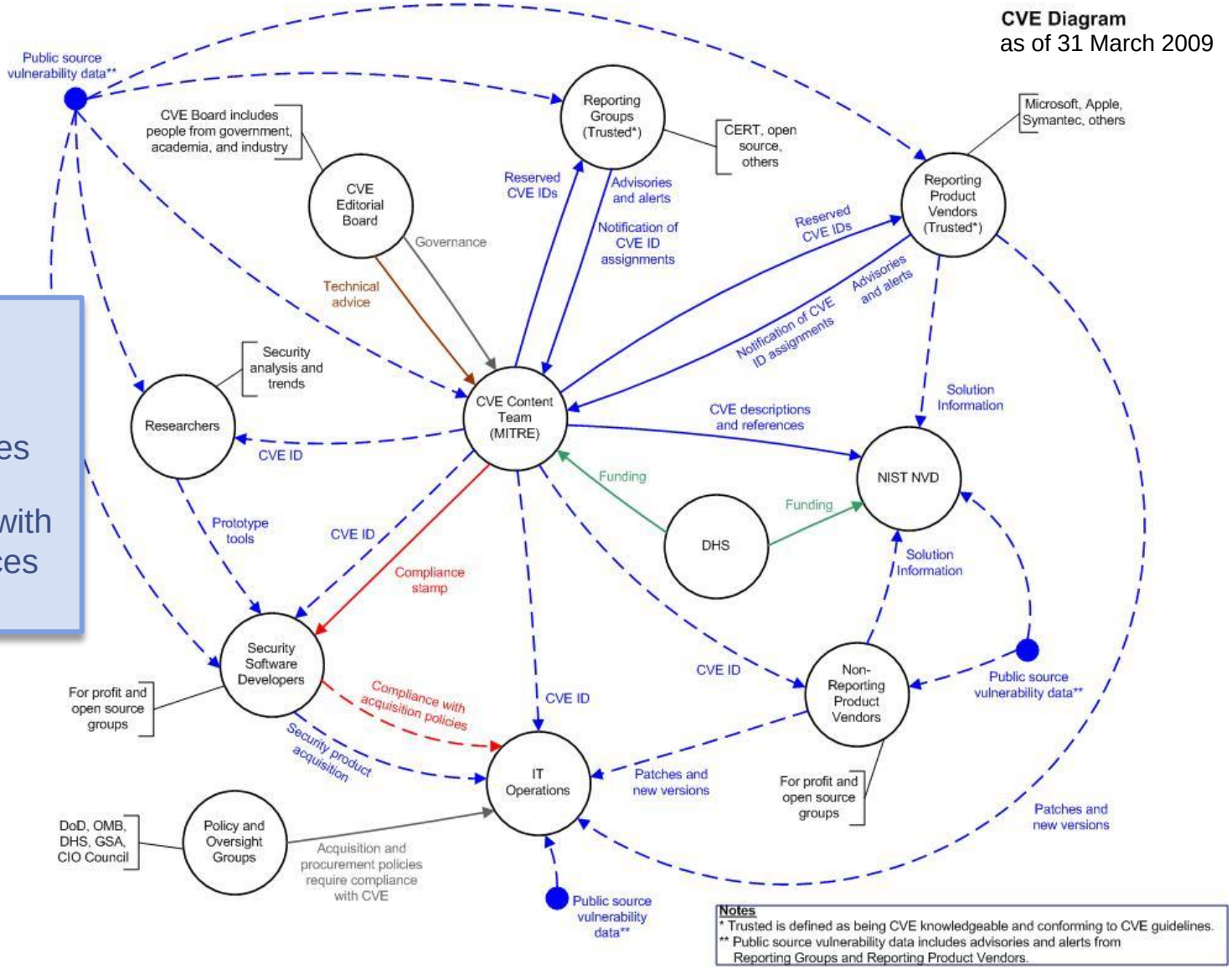
Partial CVE Diagram – Notation Example



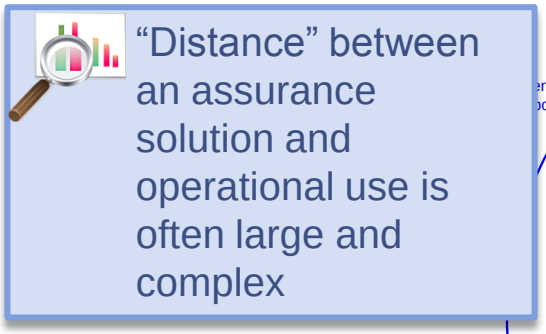
Supplying CVE

Independent organizations collaborate with minimal formalities

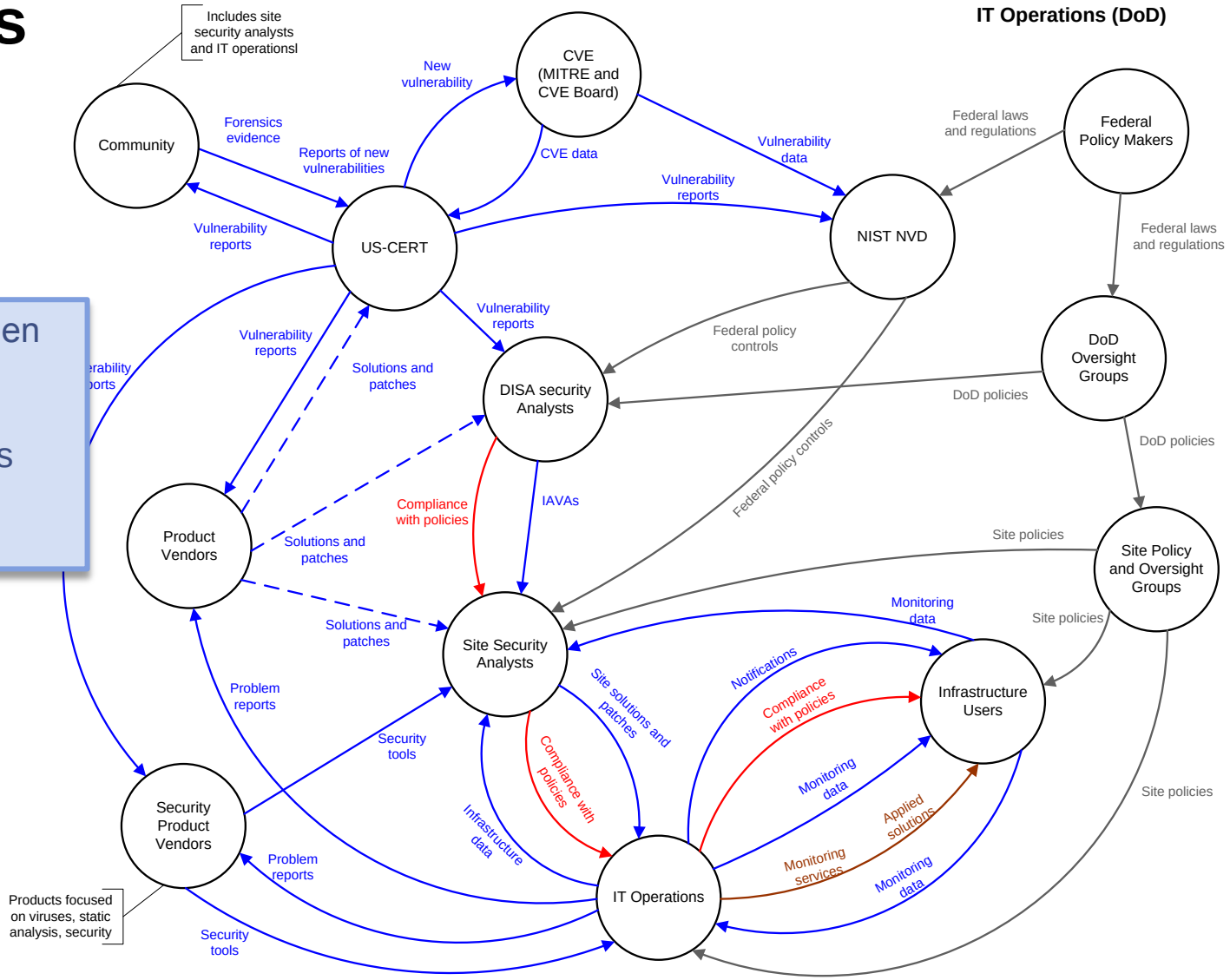
We are working with networks or lattices of relationships



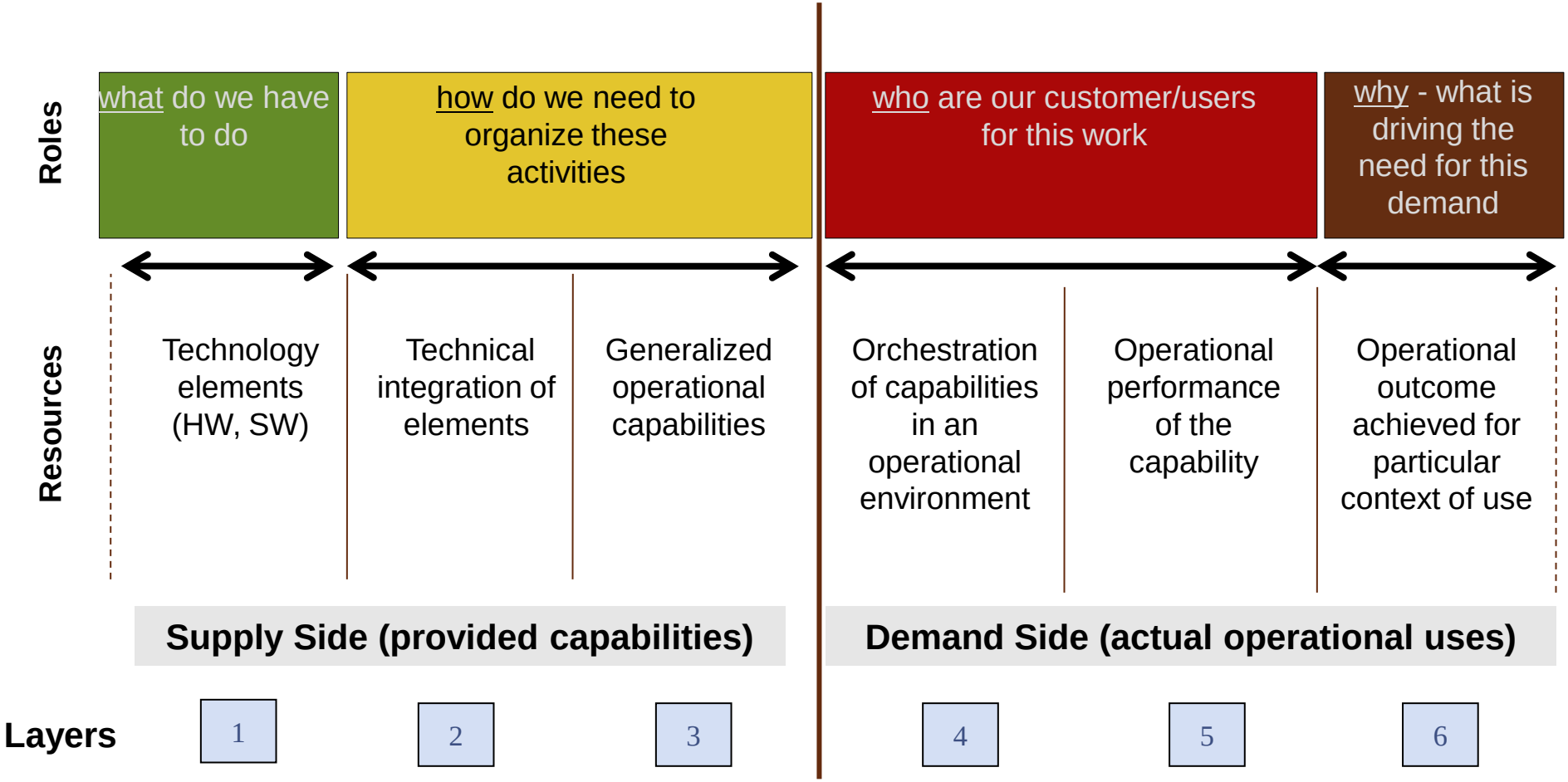
CVE for IT Operations



"Distance" between an assurance solution and operational use is often large and complex



SoS Focus Analysis: Potential Assurance Results (Q2, 4)



Permission to use PAN technology in SoS Focus Analysis is under license from Boxer Research Ltd.

SoS Focus Analysis for CVE

Strong emphasis on supply-side assurance solutions.

Areas of potential inefficiencies: where tacit knowledge is held and people manually synthesize significant information from multiple sources.

	What	How	Who	Who	Why
Roles	Vendors	CVE, NVD	Security analysts	Computer installations & operations	User environments
Responsibilities	*Addressing known vulnerabilities*	*Disseminating vulnerabilities and patches*	*Maintaining current knowledge of vulnerabilities and patches*	*Maintaining current knowledge of available patches & site configurations; forming site solutions*	*Maintaining awareness of risks and effectiveness of solutions*	*Operational assurance in the context of use*
Resources	Building, testing, issuing patches	Registering	Monitoring	Tracking, analyzing, forming solutions	Installing solutions, monitoring effectiveness	Operational availability and integrity
	Supply Side			**Demand Side**		
Layers	1	2	3	4	5	6

Polling Question 3

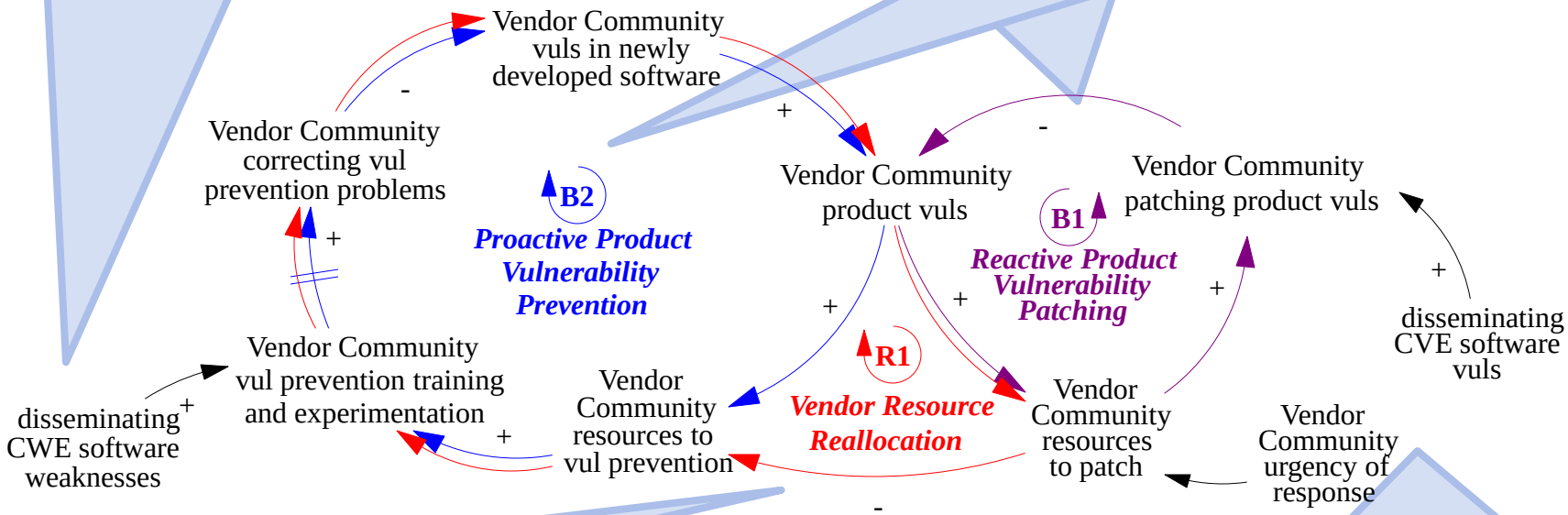
How would you characterize the focus of your organization?

a) Supply Side
b) Demand Side

System Dynamics: Critical Behaviors (Q6)

3. The proactive approach focuses on a strategy of vulnerability prevention based on applying CWE information within the vendor community to developed software that prevents vulnerabilities.

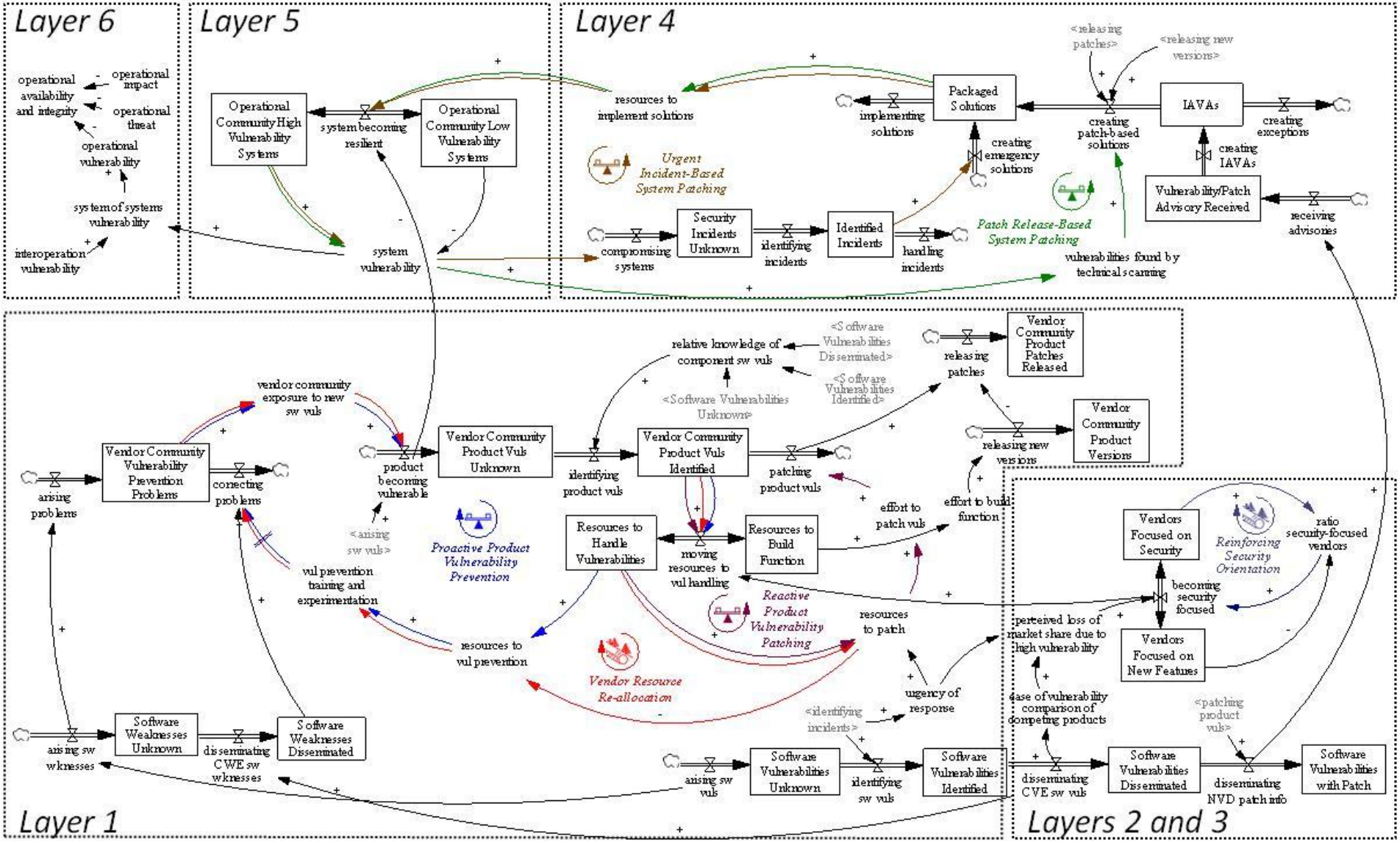
1. Vendors must decide how to split resources between reactive and proactive responses to product vulnerabilities to balance the need for an immediate response with the need for a proactive solution that prevents product vulnerabilities.



4. If vendors feel the need to devote more resources to vulnerability patching and less to vulnerability prevention, then this leads to a downward spiral of increasingly vulnerable products and ever increasing assurance problems.

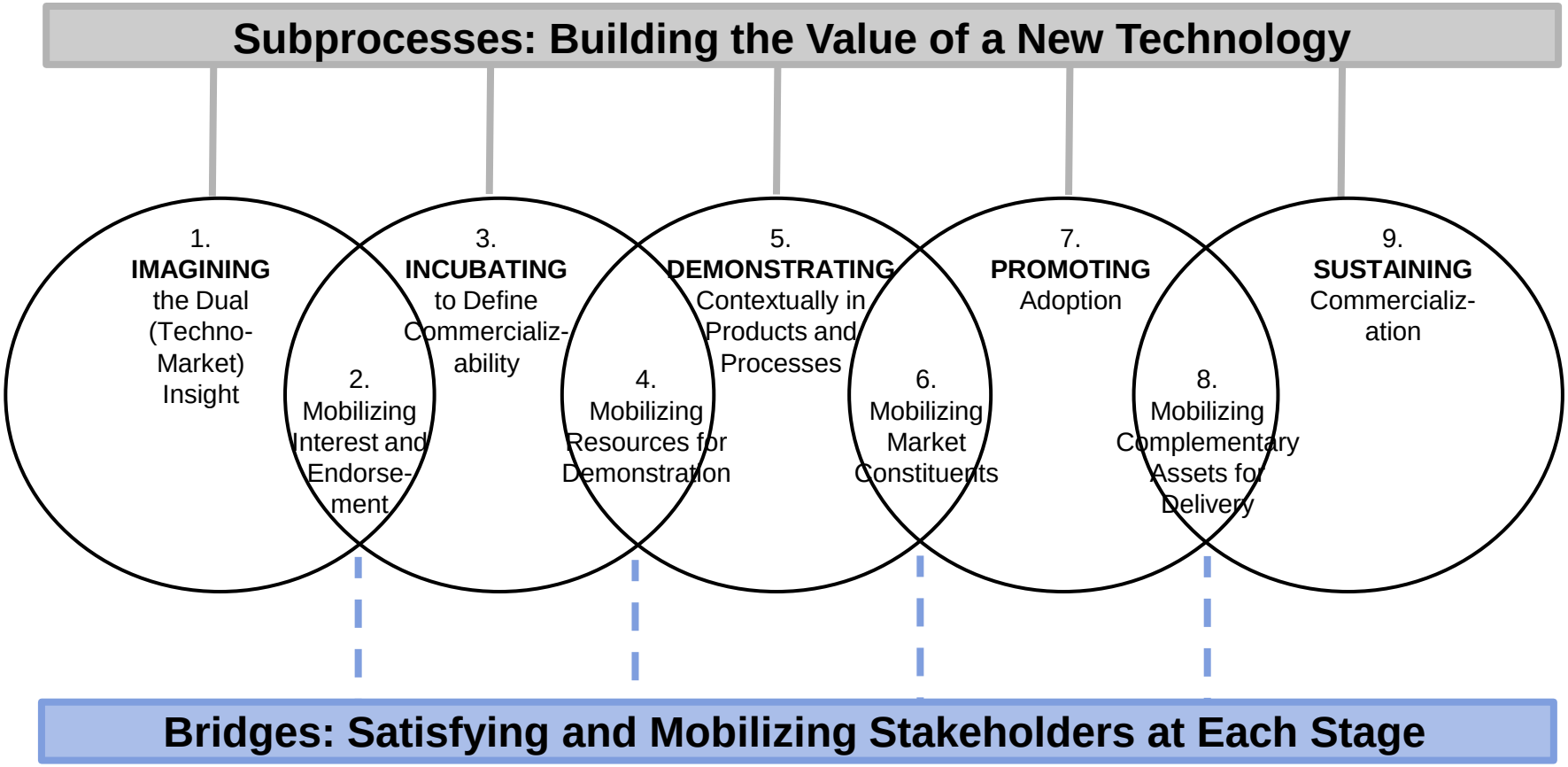
2. The reactive approach patches product vulnerabilities based on CVE information. The development of patches is prioritized based, in part, on the impact a given vulnerability is having on the operational community.

Detailed System Dynamics Model



Transition Analysis: Adoption of Products (Q7)

Issue—maturation and transition models built for single technologies and not clusters of technologies



Source: V. Jolly, Commercializing New Technologies: Getting from Mind to Market, 1997.

Extracted Success Indicators

What does success mean for assurance solutions? Market share? Improved operational assurance of some % of operational organizations?

Indicators of Maturation and Adoption Success for CVE
CVE is accepted throughout the supplier community.
CVE is considered a de-facto standard by the community.
Vendors advertise that they are CVE compliant.
Content providers/list makers reference vulnerabilities using CVE.
NVD explicitly uses CVE.

Factors Contributing to Success for CVE
MITRE identified a clear market need (from a community perspective).
Vendors were motivated to participate.
MITRE's strategy allowed it to partner with researchers and content providers/list makers.
A growing amount of vulnerability information was distributed across multiple databases (operated by competing groups).
MITRE filled an unmet community need with CVE.
MITRE signed agreements with vendors to get information earlier.
MITRE's proof of concept using public data convinced vendors of the value of the CVE approach.
MITRE identified the right stakeholders and did a good job of getting them involved in building the solution
MITRE explicitly focused on reducing the barriers to adoption
MITRE's solution did not force adopters to change the way they did business.
Government policy – DoD IAVA was rewritten to include CVE.
MITRE continues CVE "marketing" and product evolution.
There is continued investment in infrastructure.
Community articulated "standard" before MITRE used the term.
Focus on building collaborations.

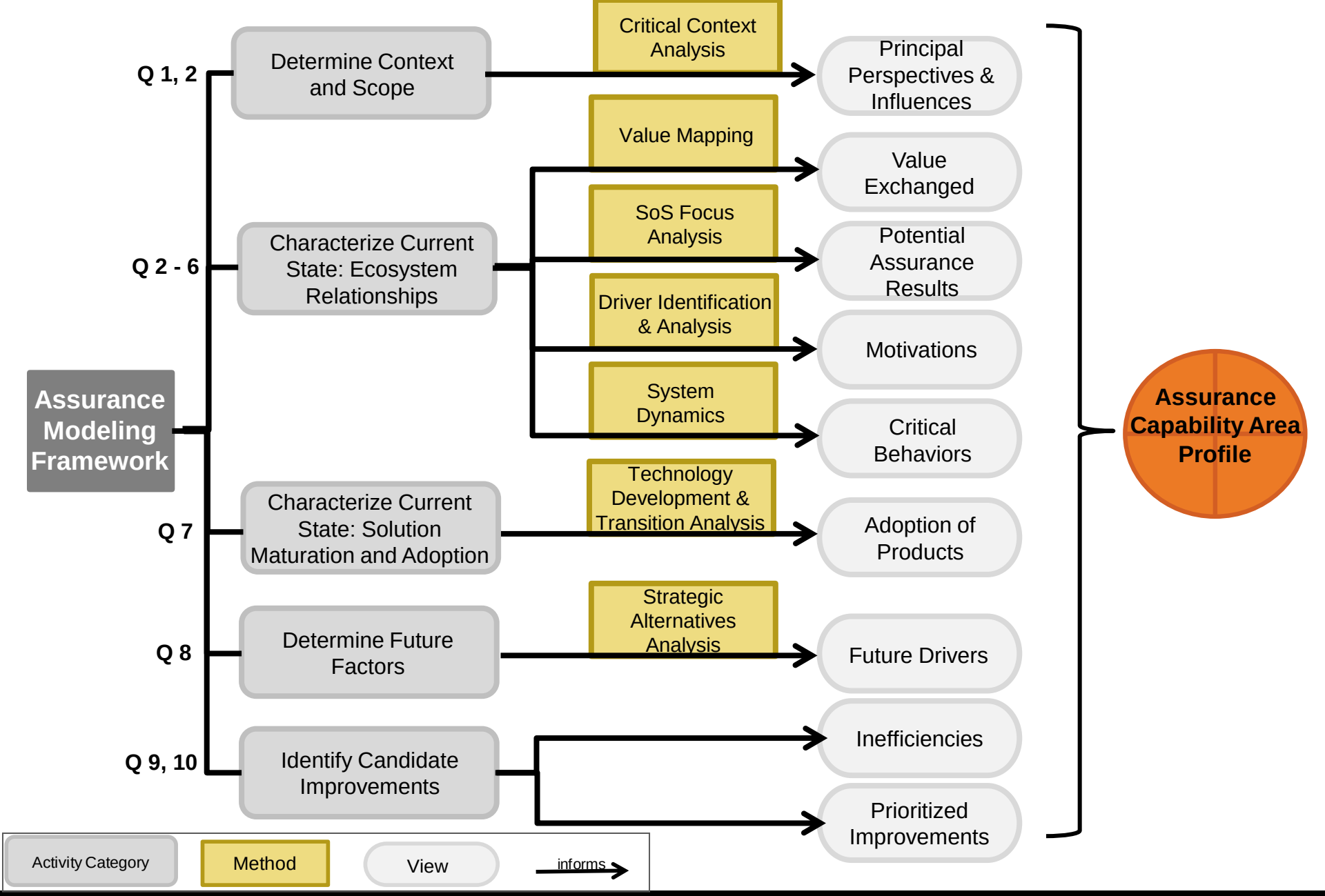
Transition Analysis Insights

Technology maturation and transition mechanisms for CVE are being applied to CWE

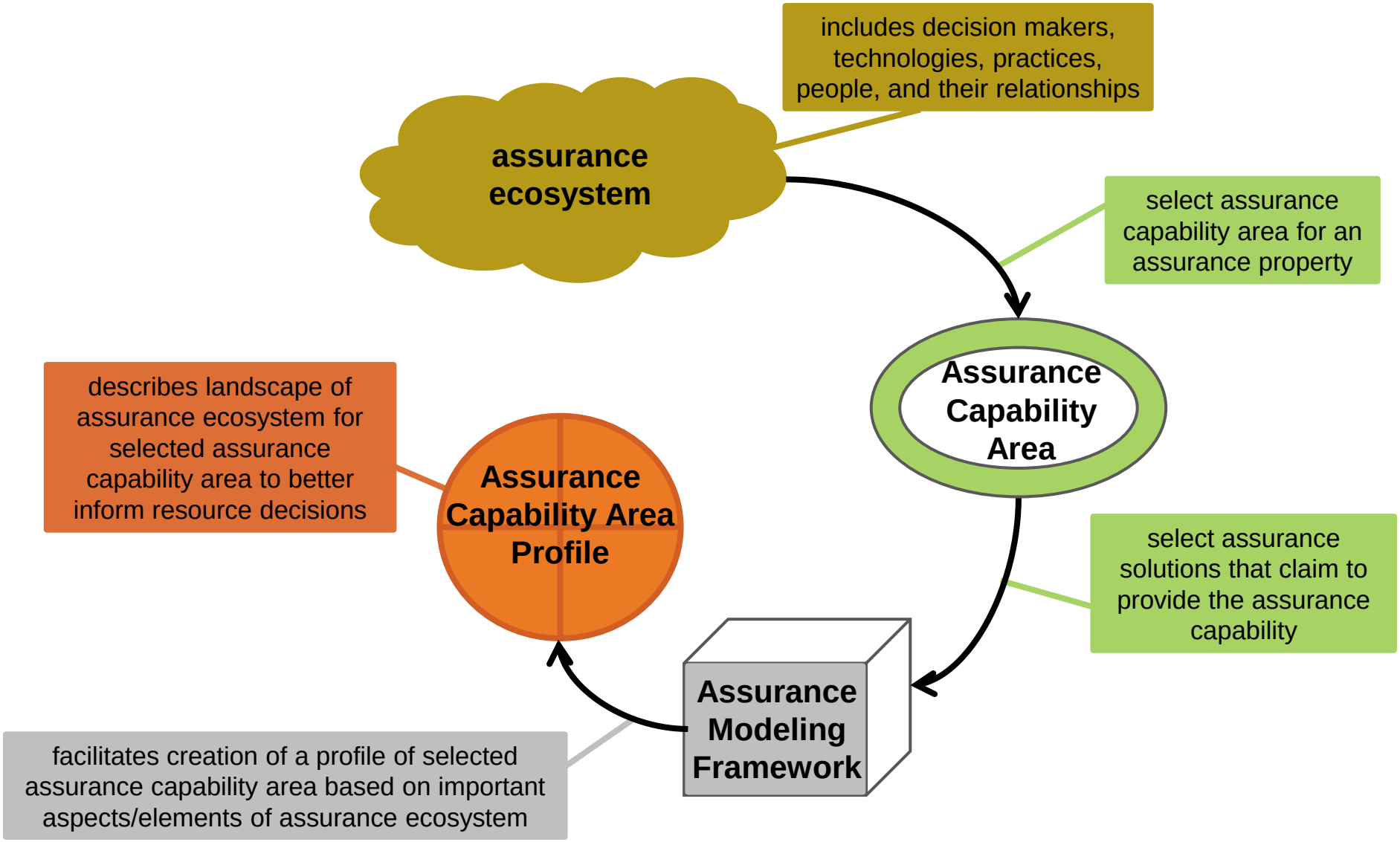
- CVE required little behavioral change on the part of its primary users (e.g., suppliers of IT and vulnerability management products)
- CWE will require extensive behavioral and process changes on the part of its primary users (e.g., software development organizations)

There are other critical differences among the user communities

- CVE: characterizes vulnerabilities from an *operational* perspective—written in the language of operations
- CWE: characterizes weaknesses associated with vulnerabilities from a software *development* perspective—written in the language of software engineering



Applying the Assurance Modeling Framework



Value of this Work

Modeling addresses key questions

- Where are the critical gaps in available assurance solutions?
- Where should resources be invested to gain the most benefit?
- What additional assurance solutions are needed?
- Are the incentives for routinely applying assurance solutions effective?

Assurance modeling framework lays important groundwork by providing a multi-dimensional approach to

- Understanding relationships between organizations and assurance solutions—how these relationships contribute to operational assurance
- Identifying potential areas for improvement across a spectrum of technical and organizational areas

Polling Question 4

Would this modeling approach be useful to your organization?

a) Very useful
b) Somewhat useful
c) Not at all

Current Work

Detailed report of framework and its pilot application to vulnerability management under final review (available summer 2010)

Apply the framework to a second assurance capability area

- Selected malicious software prevention and management
- Expand understanding of the customer/user (i.e., the demand side)

Conducted interviews and constructed initial models from the demand side

- Information Security Office
- IT operations
- CSIRT

NO WARRANTY

THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

Use of any trademarks in this presentation is not intended in any way to infringe on the rights of the trademark holder.

This Presentation may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

This work was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

Questions?

Contact Information

Lisa Brownsword
Senior Member, Technical Staff
Research, Technology, and System Solutions (RTSS) Program
+1 703-908-8203
llb@sei.cmu.edu

Carol C. Woody, PhD.
Senior Member, Technical Staff
Networked Systems Survivability (NSS) Program
+1 412-268-9137
cwoody@cert.org

Christopher J. Alberts
Senior Member, Technical Staff
Acquisition Support Program (ASP)
+1 412-268-3045
cja@sei.cmu.edu

Andrew P. Moore
Senior Member, Technical Staff
Networked Systems Survivability (NSS) Program
+1 412-268-5465
apm@cert.org